The Hashemite Kingdom of Jordan

Ministry of Digital Economy & Entrepreneurship

Cloud (Platforms & Services) Policy 2020

Table of Content

1- Foreword

(1) Over the past years, the world has witnessed an increasing rate of investment in technological equipment due to steady technological developments and consequently the costs of expanding the construction, modernization, maintenance and operation of data centers have become very expensive. So that was a key driver to motivate technologies companies to find alternative solutions for making a qualitative shift in providing technological solutions through enabling leasing of infrastructure, platforms and technological software instead of expanding the investment in building and developing data centers and purchasing software. This solution directs governments to focus on managing their technological resources effectively by adopting cloud technology, which provides the ability to expand with high flexibility, achieving better results with less administrative effort and providing e-services to all beneficiaries faster. In addition, to develop skills, saving costs, and provide an appropriate environment to create new opportunities for innovation that in turn promotes the growth of the digital economy.

(2) Therefore, governments all over the world have start adopting their own cloud model. Despite the diversity and difference in application between countries, it is certain that this will have a positive impact on the economic and social aspects. Similarly to other governments activities, the Jordanian government recognizes the need to define a clear direction for the future of cloud in Jordan, in order to achieve the goals set in national policies within the priorities of Government priorities for action 2020-2021 to develop the digital infrastructure, and reap the benefits of adopting cloud to support and develop the digital economy in Jordan.

(3) The increased adoption of cloud by government will encourage the growth of SMEs and facilitate their participation in global markets, which will fast the growth of local digital businesses and increase their contribution to the growth of the Jordanian digital economy. Beside to that the increasing use of smart technology that worked on cloud will enable government entities to develop new digital solutions and services and provide them for citizens and their partners in an innovative way to improve public services. In addition to it will promote digital transformation by enabling government to design and manage jobs supported by information technology with more flexibility and innovation and Saving costs by taking advantage of technology resources on a "pay-as-you-go" basis which is one of the most cost-effective options for government entities.

(4) In line with the General Policy for the Information & Communications Technology and Postal Sectors (ICTP) 2018, article No. (8) which stated "… to seize the opportunities of the Fourth Industrial Revolution with the primary goal being the development of a digital economy leading to renewed economic development and increased income and wealth of individual Jordanians..", and article No. (147) of that policy stated that "Government will use cloud services to expand Government-owned storage capacity and to benefit from the data management and application services available in the cloud", Therefore, the Jordanian government, through the Ministry of Digital Economy and Entrepreneurship (**The Ministry**), decided to issue Jordan Cloud Policy, in cooperation with partners and stakeholders, and in line with the national policies and goals mentioned above. in addition to consider a cloud as one of the basic digital technologies for digital transformation.

(5) Since 2014, the Jordanian government, through the Ministry, has created and developed a Government Private Cloud (GPC) to provide a set of basic cloud services to government entities represented in the following main service Categories: Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Currently, the Ministry is providing government entities with various cloud services such as: Databases as a Service, Email as a Service, Rapid Software Development as a Service and others. In addition to servers hosting service for enabling government entities to host their servers in the government data center which belongs to the Ministry for taking advantage of the secure infrastructure, , government entities are fully responsible for the server settings, operating programs, applications used, security and updates. Beside to that, The Ministry constantly develop that infrastructure to serve a larger number of government entities in addition to develop Disaster Recovery (DR) Site. In addition, some government entities take advantage of public cloud services for some applications that do not require data at a high level of classification.

(6) As for local public cloud, in Jordan, there are private local cloud service providers that are able to provide all types of cloud service, which cover basic forms of cloud, such as Human Resources systems, email service, and data archiving that use their local cloud network, among others. Currently the cloud service providers are not regulated yet, and there is a need to have unified standards to regulate cloud service providers for ensuring quality of service and the right of the beneficiaries from either public sector, private sectors or even individuals.

2- Overview of Cloud

(7) There are many internationally approved models for managing and using cloud services, which include the following:

1. **Public Cloud:** This model provides a cloud infrastructure for public use over the Internet. The use is not limited to institutions or government agencies only, it may be owned, managed or operated by a commercial or academic company, or both. This model has group of advantages such as low service and maintenance costs and rapid scalability.
2. **Private Cloud:** It is a model that provides the cloud infrastructure for exclusive use by one party. It is managed and operated by the same party or outsourced to a third party, and it may be located on or outside the workplace. This model is characterized by maintaining the confidentiality of the data and the systems that entity deals with.
3. **Hybrid cloud:** It is a combination of public and private clouds for independent entities, but they are linked to each other through special technologies. This allows the transfer of applications, systems and data with high classification levels and store them within the private cloud, while there is possibility of using the public cloud for data and systems with medium and lower classification levels.

(8) Cloud services can be provided through one of the following categories:

1. **Infrastructure as a Service (IaaS):** The beneficiary can utilize processing, storage, networks, and other fundamental computing resources where the beneficiary is able to deploy and run arbitrary software, which can include operating systems and applications. However, the beneficiary does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of some networking components such as firewalls.
2. **Platform as a Service (PaaS):** The cloud infrastructure is beneficiary-created or uses acquired applications created using programming languages and tools supported by the provider. The beneficiary does not manage or control the underlying cloud infrastructure including networking, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
3. **Software as a Service (SaaS):** The beneficiary can use the provider's software applications that ran on cloud infrastructure. The applications are accessible from various beneficiary devices such as a web browser. However, the beneficiary does not manage or control the underlying cloud infrastructure. This service category can include the following examples accounting software, email, document management tools… etc.

3- Policy Objectives

(9) Through this policy, the government mainly seeks to build and develop an integrated ecosystem for the Jordanian cloud in a way that contributes to the growth of the digital economy through achieving the following goals:

1. Encourage government entities toward optimal use of cloud services.
2. Continue the development of government private cloud, keep pace with the latest technological developments, as achievement of the government's digital transformation plans, and ensure the availability of needed resources.
3. Ensure protection of cloud services users' by establishing a regulating framework and defining roles, responsibilities and obligations for ensuring basic protection of beneficiaries' rights and interests via cloud service providers.
4. Achieving fair competition among cloud service providers.
5. Promote the growth of local SMEs, facilitate their participation in the global market, and support the growth of cloud markets in Jordan

4- Scope of Policy

(10) This policy shall apply to:

1. All government entities that benefit from the cloud services provided, whether from the government private cloud or the public cloud locally or globally.
2. All Cloud Service Providers (CSPs) who provide cloud services to the beneficiaries either from public sector or private sectors and individuals.

(11) This policy can be considered a reference document for all other sectors that benefit from cloud services and they are involved in the process of digital transformation in the Kingdom. In addition to, those who use the cloud in their sectors or organizations.

(12) This policy shall take effect upon its approval by the Council of Ministers where the Ministry will be responsible for following up the implementation of the policy, reviewing, amending and updating it within a period not exceeding three years to keep pace with local and regional developments and best international practices.

5- Architecture of Jordanian Cloud

(13) The government is cognizant of the different characteristics and features of cloud models in terms of safety, reliability, economic cost and flexibility. Thus, Government of Jordan resolves that the architecture of the Jordan Cloud will be hybrid, as this cloud model enables it to keep pace with technological developments smoothly and quickly and ensure achieving high effectiveness in the deployment and use of services at a lower cost and in accordance with related legislation, where the hybrid cloud model includes:

1. **Government Private Cloud** – It is a model of cloud infrastructure, This cloud was established by the Ministry and owned by the Jordanian government within the Jordanian borders and it's under Ministry management and operation, dedicated for the use by government entities only.
2. **Public Cloud** – It is a model of cloud infrastructure provision for the public use, managed by Cloud Service Providers (CSP) and is wholly owned by private sector even inside or outside Jordan.

(14) The following Figure shows a Jordanian cloud architecture model. This Model is based on partnership with the private sector (local and global), which will allow to provide the cloud services to all beneficiaries from both public and private sectors and individuals according to specific controls.. Meanwhile the ministry will still work on providing cloud services to government entities through the Government Private Cloud. The Ministry shall continuously develop Government Private Cloud for ensuring the efficiency of the service and its continuing in any disasters or crises events.

6- Policy Pillars

(15) This policy covers four main pillars, which are the use of cloud services by government entities, regulating Cloud Service Providers, regulatory frameworks for cloud services providers, and Procedures and Studies to Develop the Jordanian Cloud.

(a) The use of cloud services by government entities

(16) The migration of government entities for using cloud services requires not to consider government IT as an investment in on premise applications, servers, and networks, but they shall take into account a set of considerations, including pay-per-use, terms of services, commoditized computing resources, agile capacity provisioning tools, and their enabling effect for citizens and public services. Beside to that t and not considering government information technology as an investment in applications, servers and local networks. This improves the entire IT service lifecycle, from needs identification to service operation.

(17) The Ministry and Government entities should undertake the following tasks and responsibilities for ensuring a smooth transition to the use of cloud services.

(18) **Roles and responsibilities of Ministry of Digital Economy and Entrepreneurship:**

1. Develop the Government Private Cloud to ensure the delivery of effective and safe cloud services, in addition to developing the efficiency and security of the Secure Government Network.
2. Continue to manage and provide the current cloud services in addition to develop new cloud services for government entities such as the Security as a Service (SecaaS) and Disaster Recovery as a Service (DRaaS) and data storage service (Government Drive), etc...
3. Drive government-wide adoption of cloud and share best practices and reusable example analyses and templates.

4. Ensuring capacity building and qualification of human resources and attracting expertise, competencies and specialization in the field of the cloud.
5. Facilitate migration of Government Data, information systems, and e-government functions to the Jordan Government Cloud, determining in consultation with respective Government entities the utilization of Government Private Cloud and Public Cloud components in combination, as is appropriate for specific functions, workloads, types of data, its classification level and needed capabilities.
6. Prepare the necessary guideline / instructions for government entities about using cloud services in line with this policy.
7. Spread awareness and education among government entities in the field of cloud technology through holding workshops and training courses and preparing publications and scientific documents to clarify its benefits, capabilities and requirements, and others, in order to enable government entities to determine the cloud services that cover their needs and benefit them, whether provided through the ministry or through local or global cloud service providers.
8. The Ministry continues its role as Chairman of the Committee of Organizing the Purchase of Technological Infrastructures, Computer Hardware, and related Accessories, and Software Formed by Cabinet Resolution No. (4619) (The Committee), which works to facilitate and direct the purchase of cloud services to meet the information technology needs of government agencies, whether by taking advantage of Public cloud service providers or private government cloud development services, with the importance of giving the priority to Government private cloud.

(19) Roles and responsibilities of Government Entities:

1. Government entities shall refrain from further expansion in establishing data centers or IT storage or processing infrastructure dedicated solely for the use of that government entities and shall instead utilize resources of the Jordan Government Cloud as appropriate;
2. Coordinate with **The Committee** when making decisions regarding IT procurement.
3. Adhere to the guidelines / instructions for the use of cloud services prepared by the Ministry, and it is their responsibility to ensure that their staff apply these guidelines / instructions.
4. Prepare a preliminary report on their ability to migrate to the cloud and plan steps for the moving of data, applications, hardware, software, network infrastructure, and/or other business elements and services to a cloud-computing environment. Within six months of the issuance of this policy, Government entities must submit a Cloud Readiness Assessment that to The Ministry, at a minimum addresses the following elements:
   - Accounting of current ICT systems and assets, and the functions they support.
   - Assessment of current costs and utilization gaps of current ICT systems and assets.
   - Assessment of the readiness and feasibility of migrating functions provided by current ICT systems and assets to a cloud environment, taking account of estimated cost, ease of migration.
5. Submit a final Cloud Migration Plan to The Ministry within 18 months after issuance of this policy, based on the outcomes of the preliminary report on their ability to migrate to the cloud report, which at a minimum, includes:
   - Priority systems, assets, functions and tasks that are best suited to move to the cloud.
   - Specific and time-bound targets for the migration of specified ICT systems and resources to the cloud.
   - Digital assets that are not subject to migration and the justification.
   - Outline of steps that Government entities expect to undertake to execute this plan.
6. Continue the development of Migration plans and submitted to The Ministry annually .In addition to provide Ministry with an assessment of their progress in implementing their Cloud Migration Plan before first revision of the policy, which the Ministry will do.
7. Classify their assets which include data, equipment, and software that will be transferred to cloud in accordance with the Data Classification and Management Policy of government 2020, before taking advantage of the solutions cloud. These considerations shall be reflected appropriately in contracts and agreements with CSPs. The following is an explanation for each classification level:

- The first level (**Secret**): then the place of preservation and processing is limited within the Kingdom to the secure data centers in the government with the possibility of restrictions, and the authority can benefit from all the cloud services.
- The second level (**Sensitive**): The place of preservation and processing is limited within the Kingdom, with the possibility of utilizing the secure data centers in the government with all different cloud services, and the secure data centers in the private sector with the possibility of restrictions. So, Government entities can take advantage of SaaS cloud services only.
- The third level (**Private**): The place of preservation and processing can be inside or outside the Kingdom, with the possibility of taking advantage of secure data centers in the government and the private sector with all the different cloud services, with the possibility of restrictions on data centers in the private sector and / or outside of Jordan.
- The fourth level (**Ordinary**): The place of preservation and processing can be inside or outside the Kingdom, with the possibility of benefiting from the secure data centers in the government and the private sector, and all different cloud services can be used.

Additional restrictions in the above classification such as encryption, tokenization, anonymization, data decomposition, and implementing cyber deception defense solutions shall ensure that data is not seen, accessed and replicated in the cloud by local or global cloud service providers.

8. When contracting with a cloud service provider outside Jordan, their data centers must be in countries whose legislative and regulations related to the privacy and personal data protection comply with the relevant Jordanian legislation and regulations.
9. Government entities that enter into an agreement with a CSP shall determine the level of data security and protection that meets the security needs and requirements of government data that will be preserved and processed by the Cloud Services Provider in accordance with the government data classification and management policy for the year 2020, and the instructions and procedures issued by it, as a reference for the restrictions and technical security controls that must be available to preserve, process, circulate and destroy each level of classification, and to the Cybersecurity Law No. (16) -2019 and the legislative and executive frameworks issued by it, in addition to Personal Data Protection Law (when issued).

(b) Regulating Cloud Service Providers

(20) For the purposes of ensuring the protection of beneficiaries and achieving fair competition between cloud service providers, the Telecommunications Regulatory Commission (TRC) and Cloud Service Providers (CSPs) undertakes a set of roles and responsibilities outlined below.

(21) **Roles and responsibilities of Telecommunication Regulatory Commission:**

The Communications Law No. (13) of 1995 and its amendment entrusted a set of roles and responsibilities for TRC which related to regulating the provision of telecommunications and information technology services in the Kingdom in accordance with the established General Policy for the Information & Communications Technology and Postal Sectors to ensure the provision of that services to beneficiaries at a high level and reasonable prices in a manner that achieves Ideal performance for the telecom and information technology sectors, therefore, the TRC shall be responsible on the following:

1. Issue regulations and regulatory requirements for Cloud Service Providers including instructions, guidelines, standards, mandatory terms, service level agreements (SLAs) and contracts, managing the certification approval of Cloud Service Providers, And any other related instructions in coordination with the concerned authorities to ensure the growth of the Jordanian cloud market and fair competition between CSPs.
2. Conduct periodic audits of CSPs to ensure compliance with all cloud regulatory requirements in addition to periodic reviews of CSPs in accordance with the mechanism it considers appropriate by TRC which can be done in collaboration with third party.
3. Requesting information and periodic reports from cloud service providers on various matters related to the provided services.

4. Determine the minimum main terms and conditions, in accordance with the relevant international considerations and standards, that must be met by contracts and service level agreements signed between the CSPs and the beneficiaries, whether they are public sector, private sector, or individuals.

(22) **Roles and responsibilities Cloud Service Providers:**

1. Cloud Service Providers (CSPs) are responsible for providing services in accordance with legal and contractual obligations and agreed SLAs with beneficiaries at all times.
2. Comply with the regulatory requirements issued by the authority, including preparing contracts and service level agreements in line with the regulatory controls for cloud service providers mentioned in this policy then submitting them to the authority for approval before signing them with beneficiaries.
3. Notify TRC, the Ministry and the beneficiary of any data violations or any technical defect that occurs to the provided services in accordance with the contract and SLA that were complied with the TRC's controls for this purpose.
4. CSP must not enable any person or entity to access data without the prior clear approval from concerned beneficiary. In the event that the CSP desire to contract with a third party, the CSP must obtain the prior approval of that by concerned beneficiary and sign a non-disclosure agreement with the third party to ensure the security of the data and systems.

(c) Regulatory controls for cloud services providers

1. Contracts

(23) Contracts between the beneficiary and CSPs must include the following minimum requirements:

1. Full description of services to be provided; the contract's duration; payment terms and termination.
2. Details on the Service Level Agreements (SLAs).
3. CSP's customer care services depending on a service offering.
4. Beneficiaries' rights to retrieve their data stored in the CSP's system, if the cloud contract is terminated, in line with related legislations.
5. Restrictions on cloud service providers if their responsibilities are unacceptably excluded or the terms of the contract are unfairly exploited, for example, damage to or loss of data, deterioration in service quality; lack of service or data breach.
6. Return / back out plan for using cloud services.
7. Cases that require changing cloud service providers and moving to a second provider for these services.
8. Penal conditions.
9. Cases where one of the parties is entitled to terminate the contract by the service provider or the beneficiary.

2. Service Level Agreements SLAs

(24) SALs must include a set of key undertakings when signing contracts with CSPs, as follows:

1. Availability and timeliness of services.
2. Business continuity including disaster recovery, contingency and risk plans and Help Desk Support.
3. Security standards compliance, vulnerability and penetration management.
4. Confidentiality and integrity of data, and data protection compliance, including Backups, retention periods, rights of the data subject and Encryption Controls; Access, management and data controls Permissions.
5. Physical Data location.
6. Right to change the cloud service provider and moving to a second cloud service provider.
7. Mechanism for storing and processing beneficiaries' data.

3. Network and Information Security

(25) CSPs must comply with regulatory requirements related to information and network security, maintain the utmost integrity of information systems and beneficiaries' data, and meet information security requirements, and data may not be stored, shared, processed, used, disclosed, disrupted, modified, or destroyed in any way that would. Violating data integrity. The cloud service provider is also obligated to protect the data from unauthorized access. Cloud service providers are not allowed to access or

monitor the beneficiaries 'data, and they must fully adhere to the level of confidentiality required by the beneficiary.

(26) CSPs shall respond to changes that may occur in the cloud network security instructions and take appropriate measures to implement them, and the implementation mechanism should be quick and urgent in the emergent and sensitive changes cases' according to the decisions of TRC and other authorities related to cyber security.

(27) CSPs shall inform the beneficiary and TRC of any data breach or technical defects in the services provided in accordance with the contract and data, or any technical defect in the services provided in accordance with the contract concluded with it, and TRC shall coordinate and notify the concerned authorities with cyber security.

(28) within one year of the date of the adoption of this policy, TRC, in consultation with the concerned entities, should prepare a guidance document on information security in the cloud based on the National Cyber Security Policies, as this document should define the general principles of beneficiary information security that are stored, transferred, and processed in the cloud systems for clarifying all obligations of cloud computing service providers in information security and ensure that the data retained in cloud computing services is effectively protected.

(29) TRC shall coordinate with Cybersecurity concerned authorities to issue and certify cloud information security certificates. Cloud information security certification accreditation programs must provide transparency and the ability to verify CSP's compliance with information security practices and approved networks through their review and evaluation processes specialized independent third parties. Beneficiaries of the cloud services can take advantage of these certificates to ensure that they meet the major and necessary security requirements such as the provision of means of monitoring and response all the time in addition to providing specialized systems to communicate data to authorized persons.

(30) Among others, Cloud Information Security certificates can be based on a set of international standards in addition to the standards issued by TRC within the regulatory decision.

(31) Government entities must conduct a risk assessment resulting from outsourcing the services to the cloud services provider, evaluate the agreements concluded for that, periodically update them, and add them to the entity's risk assessment record.

4. Information Privacy

(32) Personal data held, transferred, or processed by a CSP on behalf of the beneficiaries must ensure the protection of this data against unauthorized access, use, disclosure, disruption, modification or destruction in accordance with all requirements of Jordanian personal data protection law and related legislations.

(33) CSPs are responsible for providing services in accordance with the contractual obligations at all times. CSPs must not have access or the capability to monitor beneficiaries' data and content, maintaining a strict adherence to the level of confidentiality that beneficiaries require and they should implement required technical and security controls and measures such as encryption or anonymization to protect data whether data is stored or being transferred.

(34) CSPs shall be compliant with any cloud personal data protection, and personal data protection certification standards can be based on a set of international standards in addition to the standards issued from the Ministry within personal data protection law (when issued).

(d) Procedures and Studies to Develop the Jordanian Cloud

(35) In order to developing and enhancing the competencies & skill related to the cloud, The government requests the Council for the Development of Professional and Technical Skills to be formed under the Law on the Development of Professional and Technical Skills No.(9) of 2019, the need to work on studying and identifying the required cloud skills locally and globally in cooperation with the Ministry, in order to determine the education needs and skills that are expected, in addition to the basic skills that the Jordanian workforce needs to adapt to labor markets that are depend on cloud services and priority areas to acquire high technical skills to support research, development and design in the cloud domain.

(36) The Ministry should study the possibility of developing the software used to create the cloud network locally and rely on open source software and develop it. To achieve this, a strategic partnership can be undertaken with Jordanian universities and educational institutions to direct their students to work projects that serve the private government cloud and contribute to building their infrastructure by relying on open source software.

(37) The Ministry should Keep up to date and follow up on the technical developments related to Quantum Computing technology and study the possibility of using this technology in the future to serve the government private cloud. In addition to keep abreast of and follow up on the technical developments related to Internet of Things (IoT) technology and Big data and prepare to provide the necessary infrastructure to support these technologies such as: Fog and Edge Computing Service.

(38) The Ministry should study the possibility of establishing a government electronic store for cloud applications in order to facilitate access to cloud applications by users, ensure software security, and provide technical support, and issue modifications and developments to this software.

(39) The Ministry must study the feasibility and effectiveness of the possibility of linking data centers in government entities with each other and launch a unified cloud network that depends on Grid Computing technology. If the feasibility and effectiveness of the study is proven, the Ministry will create a mini network consisting of group of data centers as a prototype (Pilot Study) for the purposes of proving the feasibility and identifying the lessons and lessons learned for use in developing appropriate plans.

(40) The government also encourages cloud service providers from local companies that provide cloud service based on clean (green) technology in addition to innovative solutions in the management of cloud services